Unveiling the project fAcilitating Public & Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts – APPRAISE: the future for preventing and providing security for soft targets

Sónia M. A. Morgado
Tiago Nabais
Sérgio Felgueiras

Introduction

Since the dawn of time, the path of humanity has been followed by the need for security in numerous fields. Globalisation as an apparently irreversible process (Morgado, 2013a) incarcerates constant challenges and changes that influence strategic decisions (Morgado & Felgueiras, 2021), whether in law enforcement agencies (LEAs), security policies or counter-terrorism approaches. Regardless of "the dynamics of the geo-strategic, geo-political, geo-territorial, and geo-criminal contexts", security "is a vital public good and a fundamental and foundational right of life in society." (Morgado & Felgueiras, 2022, p. 57).

Current experience on terrorism demonstrates that it has evolved, and from an individual or undersized scale, the proportions grew for mass scenarios that provoke impact. Its common ground that the concerns raised by terrorist attacks at shopping malls (Copenhagen2022; Munich 2016, Minnesota 2016), airports (Domodedovo 2011, Brussels 2016, Istanbul

2016, Lauderdale, 2017), transport systems (Madrid, 2004; London, 2005; Moscow 2010, Brussels 2016), squares and streets (Wall Street 1920. Paris 2015, Berlin 2016; Nice 2016, Barcelona 2017, Stockholm 2017; Times Square 2017, Istanbul 2022), church's (Turkey, 2024), concert halls (Moscow, 2024) and sports events (Munich 1972; Boston 2013, Stade de France 2015, Istanbul 2016) have highlighted the importance of improving public security and safety of the "new" vulnerabilities' spots and hot spots: the soft targets.

Though the phenomenon is not new, in 2015-2017, it became prominent, hightlighting the need to protect the places that are not enduringly protected. Hence, the level of security is low and is characterised by an immense concentration of people and potential mass killing (Beňová et al., 2019; Cuesta et al., 2019; Zeman, 2020). It is also a rational choice and conveys the countries' vulnerability and democracy (Asal et al., 2009; Zeman, 2020). It is a statement that allows "value-maximising (..) goals of communication and inspiration of fear" (Asal et al., 2009, p. 261).

Soft targets are also chosen by the symbolism associated with them (Cuesta et al., 2019) and considering a terrorist as a rational actor (s)he will choose an effortless attack with less time consumption, fewer resources and with maximum results. The penta-factor combination (mass gathering, high death toll, symbolism, low security, and effortlessness) proves these targets' preference, representing 46% of the attacks (Europol, 2018). Due to COVID-19, these numbers decreased (Europol, 2021).

Considering that the prevalence of terrorist attacks on soft targets is high, the question is how to protect these targets? Some theorists argue that the solution involves transforming the soft target into a hard target (Nilsson, 2018). The number of soft targets in a city is considerable, which implies a need for more resources to raise the security levels of each target, as well as interference in exercising citizens' fundamental rights.

Implementing a security fundamental as a notification (Wayland, 2014) of early signs is a different approach. This process allows the response (Wayland, 2014) to be directed at an early stage of the potential attack, namely when preparatory acts occur. The underlying active principle is the interruption of the iter criminis. Proactively avoiding terrorist threats is crucial to prevent or reduce the impact of a potential attack. To achieve this, it is necessary to predict and evaluate the risk as soon as possible. Data analysis and Big Data play a vital role in this process, helping to identify potential threats and gather intelligence to block a terrorist attack.

Therefore, intelligence is a crucial factor in preventing terrorist attacks. Comprehending the motives (racial, educational, cultural, economic, inter-generational, hate, and others) is the set for providing effectiveness in responding to criminal and terrorist activities (Morgado, 2013b). "Unfortunately, there is no perfect or impenetrable security system that can be established—no matter what the cost or inconvenience—to protect a location against a motivated intruder or terrorist" (Wayland, 2014, p. 20).

The traditional intelligence production cycle gives an action framework (Fernandes, 2014). The multiple, diverse, and increased quantity of information sources require improving the analysis and production, the linkage of the analysis of the soft targets' risk assessment, and the response. The generation of Big Data brings the discussion about 5V's model (Dijcks, 2013; Higdon et al., 2013; Laney, 2020; Schroeck, 2020) to deal with volume, velocity, variety, veracity and value towards anticipation of early signs detection. The several sources of intelligence targeting the threats against soft targets are composed of "Internet of things, machine learning, M2M, and wrapped up with Artificial Intelligence" (Morgado & Felgueiras, 2022, p. 144), amongst others.

The ubiquitous digital and cyber threats are the new challenge to risk assessment and predictive policing. Its evaluation must be done within a dynamic, methodical and conscientious process. In this sense, legitimising the developing process for hard and soft targets while maintaining the sovereignty of citizens is undoubtedly a challenge for societies. Balancing the respect for democratic values while being protected against the rise of threats and e-threats is necessary (Delpech, 2002).

The highly demanding task of ensuring security and safety in society is the main reason for delivering service to LEAs. Therefore, a trophic link is established between every sector of society and technology, which induces stimuli and systemic retroaction (Morgado & Mendes, 2016). In this sense, the project fAcilitating Public & Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts – APPRAISE, encompasses the crossover of knowledge, areas, and expertise.

A successful project acts towards favouring security within an amalgamation of Big Data and AI and emphasises the need to remove or mitigate the criminal activity. Managing risks and security is possible by increasing interoperability. It allows for consolidation, the harmonisation of procedures, and articulating of the operational and technological environment (Felgueiras et al., 2019). For the APPRAISE, this interoperability conveys

public officers and private partners within a framework for detecting, analysing, and visualising threats.

APPRAISE works on solving questions about facility, physical, information and personal security. The questions arising are i) what are the threats and e-threats?; ii) what security actions and improvements are needed?; iii) what type of security and contingency plans are appropriate? So the risk management cycle involves identifying the threats and e-threats, establishing the elements to protect and the vulnerabilities, evaluating the measures to reduce risks and reviewing the measures (ACPO, 2006) within the scope of security and safety principles (Wayland, 2014).

The growth of attacks on soft targets is consubstantiated by the appeal of causing mass causalities (Gaibulloev et al., 2012; Sandler & Enders, 2005) and killing without discrimination (Jenkins, 2001). An integrative assessment must be done to reduce uncertainty, with a multilevel enactment when intermingling with citizens and society (Morgado et al., 2023). For this set of reasons, The European Union's Horizon 2020 Research and Innovation is funding APPRAISE with more than 9 million euros.

The present paper is a theoretical work. The aim is to present the project and the research pathways for improving the security of soft targets by using technology and human sensors without revealing confidential intelligence.

The Project APPRAISE

In a joint effort, 27 organisations (research centres, SMEs, industries, law enforcement agencies (LEAs), and private security practitioners and operators coordinated by a large industrial company with a leading position in the security market (national police, municipal police, elite tactical unit), from nine countries (France, Italy, Greece, Poland, United Kingdom, Germany, Spain, Slovenia and Portugal), gathered around in this consortium to help define and create an "integral security framework that will improve both the cyber/physical security and safety of public spaces by enabling a proactive, integrated, risk-based, and resilience-oriented approach." (Cordis, 2023). This will be done through Big Data analysis, AI, virtual augmentation, and advanced visualisation to deter terrorist attacks, with the improvement of the effectiveness of police activity (Morgado, 2023; Morgado et al., 2023).

The consortium has 11 work packages that will produce 93 reports. To perform the task due to the sensitivity and confidentiality of the results, only six (6) of these reports will see the light of day and will be available

to those interested in this theme. The density of the security, side by side with the social, criminal, demographic and technological change, requires the development of tools to ensure the pro-active efficiency of LEA. This is the APPRAISE context.

From the analysis of the attacks of soft targets, common characteristics arouse i) coordination; ii) deployment tactics; iii) immediate mindfulness of being affected; and iv) lack of situational awareness. For a more precise and effective understanding of the scenario, all stakeholders must interact and collaborate to "achieve real-time holistic situational awareness, predictive competencies, zero-latency intervention" (APPRAISE, 2021).

Synergic cooperation between LEAs and private security entities forms the perfect team as mediators between crowd, technology and enabling terrorist actions in a group or lone wolf mode. This partnership is urged by the better good, of providing security for soft targets, and converging the necessary actions, in the different stages of the framework: sharing intelligence, operational coordination, federated data intelligence and training. This integral security outline will improve both the cyber/physical security and the safety of public spaces.

As the delay in recognising an attack by the crowd is a possibility, which might cause strangling in the efficiency or reaction, the communication with the crowd is a two-way involvement between stakeholders: crowd and LEAs and private security operators. From here derives the need for being a human sensor (collecting live field data) and the recognition of wearables to dangerous events.

Rendering the portfolio to acquire data, there are "CCTV systems, smart city sensors, online activity (surface web, darknet, and social media), traffic data, and any other available sensor [that] pose serious challenges" (APPRAISE, 2021). This falls into the categories defined by Feldstein (2019), which determines to be the AI surveillance techniques concerning safe cities/smart cities, facial recognition systems, and smart policing.

Exploiting the potential and effectiveness of this scrutiny of information from this gathering is only possible with the complementarity of the stakeholders, as to do "predictive analytics and behaviour analysis", with trust and transparency as to provide unbiased results (Burgess, 2020 cited in APPRAISE, 2021). The comprehensive approach to applications that respect privacy ("privacy-respecting"), artificial intelligence, and "near real-time Big Data" (APPRAISE, 2021) are the mainframe for effectiveness,

proactiveness by focusing on behavioural analysis, anomaly detection, and predictive analytics (APPRAISE, 2021).

The discussion of acquiring data from the environment reveals the need for steering and controlling AI by i) managing, transparency and fairness of the algorithms (Alikhademi et al., 2022; Bogina et al., 2021; Lepri et al., 2021; Shin, 2019, 2020, 2021; Shin et al., 2022); ii) protect individuals' privacy thru limited data collection (Ferguson, 2020; Hamilton, 2021; McDaniel & Pease, 2021; Montasari, 2023) by avoiding the black-box syndrome (Joh, 2017; Schlehanhn et al., 2015); iii) using robust data security procedures (Marquenie & Quezada-Tavárez, 2022); iv) providing transparency and accountability (McDaniel & Pease, 2021; Meijer & Wessels, 2019; Oatley, 2022; Shapiro, 2021) (for more information see Accountability Principles for Artificial Intelligence – AP4PI (AP4PI, 2022)), and, v) involving the community (Hung & Yen, 2021).

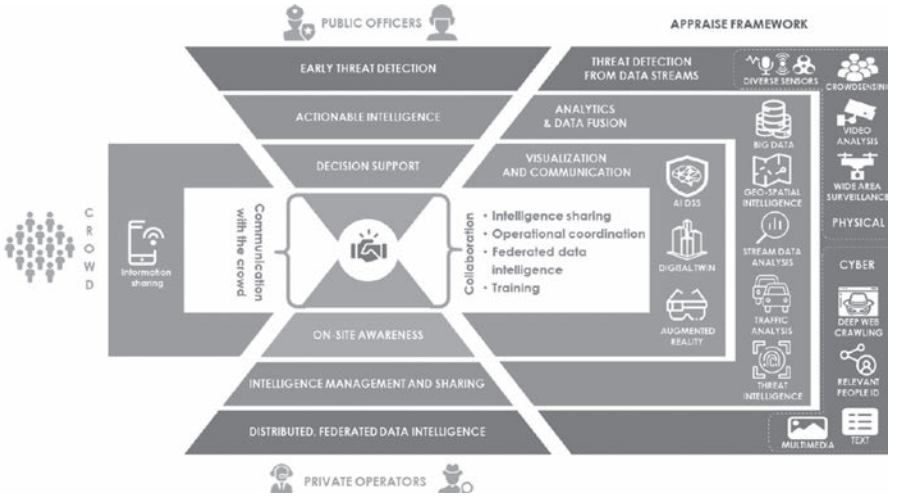
Therefore, the architectural development of APPRAISE muses those elements. Sustained by them the project aims "to revolutionise the protection of soft targets by integrating (i) a scalable, flexible, and efficient Data Intelligence platform for threat detection (dangerous objects, suspect tracking, abnormal behaviour, mobility incidents, cyber-attacks), (ii) actionable Threat Intelligence (threat analysis, public mobility analytics, geospatial intelligence, event prediction) to proactively detect vulnerabilities and analyse imminent and ongoing crimes or terrorist attacks, (iii) soft target risk assessment based on both web content, social media analysis and on-site sensor data, (iv) instant situational awareness (Digital Twin based Hypervision, AI-based Decision support, C2 integration) to plan and execute mitigation actions and (iv) collaboration capabilities (operational collaboration, federated intelligence, information sharing, crowd communication, AR-based training) to collaboratively mitigate incidents from the earliest stage of their detection (APPRAISE, 2021).

The APPRAISE framework will be co-designed with "Social, Ethical, Legal, and Privacy (SELP) experts, introducing novel approaches (edge data processing, federated intelligence, responsible AI, risk-based information sharing) to ensure compliance with EU data privacy framework, confidentiality requirements and societal acceptance" (APPRAISE, 2021).

APPRAISE has an all-inclusive, integrated, all-encompassing, and concerted approach to soft target security sustained in intelligence. Deriving from intelligent assessment of the risk is possible while assuring privacy and making decisions after analysing, correlating and sharing evidence, signals,

"data and information from smart systems (APPRAISE), outside (LEAs)", and from human sensors (Crowd-sensing) (APPRAISE, 2021). The described concept is well illustrated in Figure 1.

Figure 1 – APPRAISE Concept diagram



Note: The diagram is available in the grant agreement of the project. Adapted from 2021 APPRAISE, by CSGroup, 2021 (https://appraise-h2020.eu)

The two main contributors, LEAs and private security operators, are intertwined in this mission, from the early stage of threat detection of physical and cyber threats (e-threats) from data streams. For physical threats, apparel is set in motion, such as i) diverse sensors (audio sensors and geophones for detection of explosions or gunshots); ii) CCTV – video analysis (detection of weapons and suspicious objects); iii) crowd sensing (for gathering information from adjoining persons); and, iv) broad area surveillance – drones. As for the e-threats, some of the tools are: i) deep web crawling; ii) relevant people ID; iii) analysis of a text (e.g. posts, tweets, messages), and iv) multimedia analysis. While private security operators at this stage make the distribution and transform it into federated data intelligence, LEAs can, according to a matrix, determine the risk of the threat and e-threat. The second level of APPRAISE considers analytics, and data diffusion (Big Data, geospatial intelligence, stream data analysis, traffic analysis and threat intelligence) for actionable intelligence and predictive analytics recollected. Visualisation and communication (AI DSS; Digital twin and augmented reality) is level three. This spectrum upgrades the online

awareness and the quality of the decision because it is the critical element for a well-grounded one.

All this involves mutual collaboration (intelligence sharing, operational coordination, federated data intelligence, and training) and communication with the crowd, which are a two-way vehicle (transmitter and receptor of deviant behaviour or suspicious actions or objects).

The interoperability shown in Figure 1 is put in place in four complementary pilot soft targets: i) a mass gathering at a stadium – a tennis tournament in Italy; ii) an outdoor sporting event – a transnational cycling tour in France and Spain; iii) and exhibition and conference centre – International fair in Poland, and finally, iv) an indoor shopping centre – mall in Slovenia (APPRAISE, 2021).

In these sites, the latest technology is applied in the analysis of Big Data to promote the integral security of the soft targets.

Discussion/Conclusion

APPRAISE will go beyond and above when offering new capabilities to promote the identification and prediction of criminal phenomena. Cooperation is core in this process because the involvement of private security operators and LEAs is crucial for every event, before, during and after it.

APPRAISE priority setting has focused on the interoperability set up to enlarge the benefits package of technology integration. From a policing perspective, an essential feature of the debate about interoperability is the rationalisation and the efficiency of having private and public security, passers-by, and crowd in unison.

Among the limitations of providing a clear, more exhaustive notion of the project are the elements of reserved results, the confidentiality of the reports, and the fact that it is an ongoing project.

Acknowledgements

We would like to recognise and show appreciation to the APPRAISE Consortium for authorising us to present the project through this paper.

Financial support and sponsorship

APPRAISE project has received funding from the European Union's Horizon 2020 under grant agreement No 101021981 concerning "Secure societies: Protecting freedom and security of Europe and its citizens".

Conflicts of interest

There are no conflicts of interest because all the information provided is public.

References

ACPO (2016). Counter terrorism protective security device. NACTSO.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/934450/_Withdrawn__Shopping_Centres_Reviewed.pdf

Alikhademi, K., Drobina, E., Prioleau, D., Richardson, B., Purves, D., & Gilbert, J. E. (2022). A review of predictive policing from the perspective of fairness. Artificial Intelligence and Law, 30(1), 1–17. https://doi.org/10.1007/s10506-021-09286-4

AP4AI (2023, 22 February). Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain. https://www.ap4ai.eu

APPRAISE (2021). APPRAISE. https://appraise-h2020.eu

Asal, V. H., Rethemeyer, R. K., Anderson, I., Stein, A., Rizzo, J., & Rozea, M. (2009). The softest of targets: A study on terrorist target selection. Journal of Applied Security Research, 4(3), 258-278.

https://doi.org/10.1080/19361610902929990

Beňová, P., Hošková-Mayerová, Š., & Navrátil, J. (2019). Terrorist attacks on selected soft targets. Journal of Security & Sustainability Issues, 8(3), 453-471.

Bogina, V., Hartman, A., Kuflik, T., & Shulner-Tal, A. (2021). Educating software and AI stakeholders about algorithmic fairness, accountability, transparency and ethics. International Journal of Artificial Intelligence in Education, 32, 1-26. https://doi.org/10.1007/s40593-021-00248-0

Cuesta, A., Abreu, O., Balboa, A., & Alvear, D. (2019). A new approach to protect soft-targets from terrorist attacks. Safety Science, 120, 877–885. https://doi.org/10.1016/j.ssci.2019.08.019

Delpech, T. (2002). International terrorism and Europe. Chaillot Papers, (56), 1-55.

https://www.iss.europa.eu/sites/default/files/EUISSFiles/chai56e.pdf

Dijcks, J. (2013). Oracle white paper: Big Data for the enterprise. Oracle Corporation, Redwood Shores.

EU (2023, 10 February). fAcilitating Public & Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts. https://cordis.europa.eu/project/id/101021981. https://doi.org/ 10.3030/101021981

EUROPOL (2018). European Union Terrorism Situation and Trend Report 2018. EUROPOL.

EUROPOL (2021). European Union Terrorism Situation and Trend Report 2021. EUROPOL.

Feldstein, S. (2019). The global expansion of AI surveillance. Carnegie Endowment for International Peace.

Felgueiras, S., Pais, L. G., & Morgado, S. M. (2019). Interoperability. European Law Enforcement Research Bulletin, (4 SCE), 255-260. https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/339

Ferguson, A. G. (2021). Facial recognition and the Fourth amendment. Minnesota Law Review, 105, 1105-1210. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3473423

Fernandes, L. F. (2014). Intelligence e segurança interna. Instituto Superior de Ciências Policiais e Segurança Interna.

Gaibulloev, K., Sandler, T., & Santifort, C. (2012). Assessing the evolving threat of terrorism. Global Policy, 3(2), 135-144. https://doi.org/10.1111/j.1758-5899.2011.00142.x

Hamilton, M. (2021). Predictive policing through risk assessment. In J. L. M. McDaniel & K. Pease (Eds.). Predictive policing and artificial intelligence (pp. 58-78). Routdlege. https://doi.org/10.4324/9780429265365

Higdon, R., Haynes, W., Stanberry, L., Stewart, E., Yandl, G., Howard, C., Broomall, W., Koller, N., & Kolker, E. (2013). Unravelling the complexities of life sciences data. Big Data, 1(1), 42–50.

Hung, T. W., & Yen, C. P. (2021). On the person-based predictive policing of AI. Ethics and Information Technology, 23, 165-176. https://doi.org/10.1007/s10676-020-09539-x

Jenkins, B. M. (2001). Protecting public surface transportation against terrorism and serious crime: An executive overview (No. MTI Report 01-14). Norman Y. Mineta International Institute for Surface Transportation Policy Studies.

Joh, E. E. (2017). Feeding the machine: Policing, crime data, & algorithms. The William and Mary Bill of Rights Journal, 26(2), 287-302.

Laney, D. (2020). 3-D data management: Controlling data volume, velocity and variety. META Group. https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Lepri, B., Oliver, N., & Pentland, A. (2021). Ethical machines: The human-centric use of artificial intelligence. IScience, 24(3), 102249. https://doi.org/10.1016/j.isci.2021.102249

Litman, T. (2020). Terrorism, transit and public safety: evaluating the risks. Security World International, 8(3) 78-81.

Marquenie, T., & Quezada-Tavárez, K. (2022). Data Protection Impact Assessments in Law Enforcement: Identifying and Mitigating Risks in Algorithmic Policing. In G.

Markarian, R. Karlović, H. Nitsch, & K. Chandramouli (Eds.). Security technologies and social implications (pp. 32-60). Wiley. https://doi.org/10.1002/9781119834175.ch2

McDaniel, J. L. M., & Pease, K. (2021). Introduction. In J. L. M. McDaniel & K. Pease (Eds.). Predicitive policing and artificial intelligence (pp. 1-38). Routdlege. https://doi.org/10.4324/9780429265365

Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks, International. Journal of Public Administration, 42(12), 1031-1039, https://doi.org/10.1080/01900692.2019.1575664

Montasari, R. (2023). The Potential Impacts of the National Security Uses of Big Data Predictive Analytics on Human Rights. In R. Montasari (Ed.), Countering cyberterrorism: The confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity (vol. 101, pp. 115-137). Springer International Publishing.

Morgado S. M. A., Felgueiras S. (2021) Big Data in Policing: Profiling, Patterns, and Out of the Box Thinking. In Á. Rocha, H. Adeli, G. Dzemyda, F. Moreira, A. M. Ramalho Correia (Eds), Trends and Applications in Information Systems and Technologies. WorldCIST 2021. Advances in Intelligent Systems and Computing (vol 1365, pp. 217-226). Springer, Cham. https://doi.org/10.1007/978-3-030-72657-7_21

Morgado, S. (2013a). Going global: health organisations and networking – Information society and social media. In M. Mokryš, Š. Badura, & A. Lieskovský (Eds). Proceedings in Scientific Conference 2013 (pp. 47-51). EDIS – Publishing Institution of the University of Silina, Slovakia.

Morgado, S., & Mendes, S. (2016). O futuro numa década: Os desafios económicos e securitários de Portugal. Politeia – Revista do Instituto de Ciências Policiais e Segurança Interna. Estudos Comemorativos dos 30 anos do Instituto Superior de Ciências Policiais e Segurança Interna. Ano X-XI-XII: 2013-2014-2015, (1: Studio varia), 9-35.

Morgado, S. M. A. (2013b). Crime and socio-economic context: A framework approach. In M. Mokryš, Š. Badura, & A. Lieskovský (Eds). Proceedings in Scientific Conference 2013 (pp. 139-142). EDIS – Publishing Institution of the University of Silina, Slovakia.

Morgado, S. M. A., & Felgueiras, S. (2022). Como a (in)segurança condiciona o desporto: do grande evento desportivo à grande frustração dos adeptos na Final da Champions League 2022. SportMAGAZINE, (3), pp. 51-53.

Morgado, S. M. A., & Felgueiras, S. (2022). Technological policing: Big data vs real data. Politeia, (XIX), 139-151. https://doi.org/10.57776/hkcb-br21

Morgado, S. M. A., Carvalho, M., & Felgueiras, S. (2023). Diagnosis model for detection of e-threats against soft-targets. In A. Rocha, H. Adeli, G. Dzemyda, F. Moreira, & V. Colla (Eds.), Lecture Notes in Networks and Systems: Information Systems and Technologies - WorldCIST 2023. (vol. 1, in press). Springer Nature Switzerland AG.

Morgado, S. M. A. (2023). Inteligência artificial e metamorfose dos paradigmas: Economia na era da transformação. Congresso Nacional da Ordem dos Economistas

– Portugal e os Desafios do Presente: O papel dos Economistas e Gestores. https://www.ordemeconomistas.pt/xportalv3/file/XEOCM_Documento/74260936/file/S%C3%B3nia%20Aniceto%20Morgado.pdf

Nilsson, M. (2018). Hard and soft targets: the lethality of suicide terrorism. Journal of International Relations and Development, 21(1), 101–117. https://doi.org/10.1057/jird.2015.25

Oatley, G. C. (2022). Themes in data mining, big data, and crime analytics. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 12(2), e1432. https://doi.org/10.1002/widm.1432

Sandler, T, Arce, D. G, & Enders, W. (2008). Terrorism: Copenhagen consensus 2008 Challenge Paper. Copenhagen Consensus Center. https://www.copenhagenconsensus.com/copenhagen-consensus-ii/research

Schlehahn, E., Aichroth, P., Mann, S., Schreiner, R., Lang, U., Shepherd, I. D. H., & Wong, B. L. W. (2015). Benefits and pitfalls of predictive policing. In J. Brynielsson, & M. H Yap (Eds.). 2015 European Intelligence and Security Informatics Conference (pp. 145-148). IEEE: Manchester, UK. https://doi.org/10.1109/EISIC.2015.29

Schroeck, M., Shockley, R., Smart, J., Romero-Morales, D., & Tufano, P. (2020). Analytics: The real-world use of big data. https://www.informationweek.com/pdf_whitepapers/approved/137 2892704_analyics_the_real_world_use_of_big_data.pdf.

Shapiro, A. (2021). Predictive policing through risk assessment. In J. L. M. McDaniel & K. Pease (Eds.). Predicitive policing and artificial intelligence (pp. 185-213). Routdlege. https://doi.org/10.4324/9780429265365

Shin, D. (2019). Toward fair, accountable, and transparent algorithms: Case studies on algorithm initiatives in Korea and China. Javnost-The Public, 26(3), 274-290. https://doi.org/10.1080/13183222.2019.1589249

Shin, D. (2020). User perceptions of algorithmic decisions in the personalised AI system: perceptual evaluation of fairness, accountability, transparency, and explainability. Journal of Broadcasting & Electronic Media, 64(4), 541-565. https://doi.org/10.1080/08838151.2020.1843357

Shin, D. (2021). The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. International Journal of Human-Computer Studies, 146, 102551. https://doi.org/10.1016/j.ijhcs.2020.102551

Shin, D., Lim, J. S., Ahmad, N., & Ibahrine, M. (2022). Understanding user sensemaking in fairness and transparency in algorithms: algorithmic sensemaking in over-the-top platform. AI & Society, 1-14. https://doi.org/10.1007/s00146-022-01525-9

Wayland, B. A. (2014). Security for business professionals: How to plan, implement, and manage your company's security program. Butterworth-Heinemann.

Zeman, T. (2020). Soft targets: definition and identification. Academic and Applied Research in Military and Public Management Science, 19(1), 109-119. https://doi.org/10.32565/aarms.2020.1.10